REMARKS

In accordance with the foregoing, claims 3-7 and 9-15 are amended to improve clarity and claims 16-26 are cancelled without prejudice or disclaimer.

Claims 1-15 are pending and under consideration.

CLAIM OBJECTIONS:

In the Office Action, at page 2, claims 16-26 are objected to as being substantial duplicate of claims 3-6 and 9-15. Applicants respectfully traverse such objections.

Because claims 16-26 are cancelled without prejudice or disclaimer, it is respectfully asserted that the objection to the claims is rendered moot. Accordingly, it is respectfully requested that the objections to the claims be withdrawn.

REJECTION UNDER 35 U.S.C. § 101:

In the Office Action, at page 3, claims 5-6, 11-12, 18-19, 22, and 23 are rejected under 35 U.S.C. § 101 because the invention is directed to non-statutory subject matter.

In response, the claims have been amended in accordance with the Examiner's suggestion.

Accordingly, it is respectfully requested that the § 101 rejections to the claims be withdrawn.

REJECTION UNDER 35 U.S.C. § 102:

In the Office Action, at page 4, claims 7-12 and 20-23 are rejected under 35 U.S.C. § 102 in view of U.S. Patent No. 6,185,316 to Buffam ("Buffam"). The reasons for the rejection are set forth in the Office Action and therefore not repeated. The rejection is traversed and reconsideration is requested.

Buffam provides an encoding key that is a result of imposing a hashing function on an ordered set of false image points that have been conditioned to be non-coincident with any true image point in the original image and to be plausible impostors of the true image points. See column 12, lines 14-61. However, Buffam does not teach or suggest that the false image points are obtained by making arithmetical conversions. Rather, Buffam limits its description to indicating that false image transformation and key generation methods can include on-way

functions such as hashing.

Column 8, lines 1- 11 and column 14, lines 3- 44, of Buffam does not teach or suggest, "arithmetically converting each component of said physical characteristic information... to scramble said physical characteristic information," as recited in independent claim 7. This is because in Buffam, the false image point which is added to scramble the true image point is generated separately and individually from the true image point, and the false image point is not obtained by making arithmetical conversions to the true image point, which corresponds to physical characteristic information. Therefore, the configuration to "arithmetically converting each component of said physical characteristic information by using a predetermined function concerning said each component and a plurality of components having a predetermined relationship with said each component, to scramble said physical characteristic information" is unique to the present invention as recited in independent claims 7, 9, and 11.

Although Buffam explains that some systems apply a cryptographic algorithm to scramble (encrypt) passwords before they are transmitted, Buffam further explains that an attacker may still be able to record the encrypted password, and gain access to the host computer by submitting the encrypted value. See column 4, lines 49-56. Thus, it appears that Buffam teaches away from scrambling. Rather than "arithmetically converting each component of said physical characteristic information ... to scramble said physical characteristic information," Buffam teaches away from such recitations as recited in independent claims 7, 9, and 11.

Referring to independent claim 8, by merely providing a decoder removing true image points from information points and extracting a decoding key from false image points using the key, and comparing an original plaintext with a proffered plaintext with an authenticating signal, Buffam fails to teach or suggest, "descrambling said scrambled physical characteristic information by removing each element from each component constructing the result of decryption, in which each element is effected at the time of scrambling, by a plurality of components that has a predetermined relationship with said each component," as recited in independent claim 8.

Because independent claims 9-12 and 20-23 include similar claim features as those recited in independent claims 7 and 8, although of different scope, and because the Office Action refers to similar portions of the cited references to reject independent claims 7 and 8 and 9-12 and 20-23, the arguments presented above supporting the patentability of independent claims 7 and 8 are incorporated herein to support the patentability of independent claims 9-12

and 20-23.

In view of the foregoing, it is respectfully asserted that independent claims 7-12 and 20-23 are patentable in view of Buffam. Accordingly, it is respectfully requested that independent claims 7-12 and 20-23 be allowed.

REJECTION UNDER 35 U.S.C. § 103:

In the Office Action, at page 6, claims 13-15 were rejected under 35 U.S.C. § 103 in view of Buffam and further in view of U.S. Patent No. 5,724,427 to Reeds III ("Reeds"). The reasons for the rejection are set forth in the Office Action and therefore not repeated. The rejection is traversed and reconsideration is requested.

Buffam generally describes a comparator including a decoder that removes a claimant true image points from the information points and produces proffered false image points. See column 8, lines 28-38. The decoder extracts a decoding key from the proffered false image points using the key to decode the ciphertext therewith and produced proffered plaintext. However, the cited reference fails to teach or suggest that the decoding key is generated "for decrypting said cryptographic key, from said **encrypted physical characteristic information and** said **numeric key**," emphasis added, as recited in independent claim 1. Nothing in Buffam teaches or suggests the generation of the auxiliary code.

Referring to Reeds, this reference generally describes a method on how the information to be transmitted is to be encrypted by using a cryptographic key. Specifically, the cryptographic key to be used to encrypt a part of a plain text is changed during the course of encrypting the plain texts to be encrypted one after another, which is done by using a part of a telegraphic text, which precedes the plain text and which is encrypted beforehand by using the original cryptographic key. On the other hand, the present invention concerns a technique in managing keys, to safely hand over the key to the receiving side. From this point of view, the autokey cipher technique in Reeds does not disclose any measures to hand over the original encryption key (such as the letters "BLUE") to the receiving side.

Next, it is clear that Reeds cannot realize the characteristic of the present invention that a cryptogram, generated by combining the results of encrypting physical characteristic information and an auxiliary code using the result of encrypting, cannot be restored at all on the decrypting side, when the cryptogram is altered during the course of transmission in the network. This is not possible to do in Reeds because when the cryptogram that is encrypted by stream encryption (on which Reeds bases its invention) is altered during the course of transmission, the

information up to the point where it was altered is normally restored. This is due to the feature included in the stream encryption technique.

Moreover, because of this feature, Reeds cannot prevent replay attacks that involve alteration of a part of the information obtained fraudulently. This type of replay attack cannot be prevented in Reeds because the difference between the true physical characteristic information and false authenticating information (made by altering the last part of the true authenticating information, obtained by wiretapping and such) is mistaken. The difference is mistaken in that the difference is taken as fluctuations that appear in physical characteristic information every time it is authenticated. This results in the acceptance of replay attacks in Reeds. On the other hand, preventing such replay attacks is one of the many benefits and advantages of the present invention, and the present invention actually can achieve such benefits and advantages. Also, the feature of being able to prevent such replay attacks is a greatly advantageous feature in the field of authentication systems that utilize physical characteristic information such as fingerprints.

Thus, in view of the foregoing, Buffam and Reeds, individually or combined, fail to teach or suggest, "generating a cryptographic key from said numeric key and a predetermined primary key; encrypting said physical characteristic information using said cryptographic key; and generating an auxiliary code for decrypting said cryptographic key, from said encrypted physical characteristic information and said numeric key," as recited in independent claim 1.

Because independent claims 2-6 and 16-19 include similar claim features as those recited in independent claim 1, although of different scope, and because the Office Action refers to similar portions of the cited references to reject independent claims 1-6 and 16-19, the arguments presented above supporting the patentability of independent claim 1 is incorporated herein to support the patentability of independent claims 2-6 and 16-19.

In the Office Action, at page 8, claims 13-15 and 24-26 were rejected under 35 U.S.C. § 103 in view of Buffam and further in view of U.S. Patent No. 5,799,088 to Raike ("Raike"). The reasons for the rejection are set forth in the Office Action and therefore not repeated. The rejection is traversed and reconsideration is requested.

The "encrypting unit encrypting said physical characteristic information using said password as a cryptographic key and outputting a cryptogram," recited in independent claim 13 is based on the idea that fluctuation, which is a characteristic inherent to the physical characteristic information, is utilized in a positive way as being equivalent to the random characteristic of a cryptographic key in the process of encryption using a disposable key. As a

result, the encrypting unit recited in independent claim 13 is different from the encrypting unit of Buffam and Raike, individually or combined, in that the encrypting unit recited in independent claim 13 does not have the unit randomizing the password, which is a fixed key. Thus, it could also be said that the fluctuation in the physical characteristic information can give the same level of security as randomizing the cryptographic key because an encrypted plain text can be decrypted, as long as the text is some sort of language, by using a fixed cryptographic key and decrypted according to certain rules that language has.

On the other hand, physical characteristic information inherently includes fluctuation, and this could be taken as adding random values to each element configuring the physical characteristic information. Therefore, the cryptogram which is the result of encrypting physical characteristic information by using a fixed password is much more difficult to encrypt compared to a cryptogram of a plain text encrypted by using a password, and it is similar to a cryptogram generated by using a randomized cryptographic key.

Furthermore, the idea of complementarily using the nature of the physical characteristic information and the nature of passwords by encrypting physical characteristic information using passwords is unique to the present invention. One of the many aspects of the present invention is that passwords are much more difficult to steal because physical characteristic information, which is permanent but fluctuates as a result of measurement, is encrypted by using a password which can be managed by the user. This feature prevents unauthorized access by having the user take the initiative of changing the password, even when the basic data of physical characteristic information is stolen.

In contrast, neither Buffam and Raike, individually or combined, does not disclose or suggest that when in case the basic data concerning physical characteristic information are stolen, there is the problem that a user will not be able to use the system of being authorized by using his or her physical characteristic information, just because physical characteristic information is, by nature, permanent. Moreover, Buffam and Raike do not describe or suggest how a user can escape the situation as such, by using a password that can be managed by him or herself.

Accordingly, in view of the foregoing, it is respectfully asserted that the prima facie obviousness rejection fails on its face and, accordingly, Buffam and Raike fail to teach or suggest a trading card comprising "a proof information inputting unit inputting information including identifier or identifying the individual and a password, an encrypting unit encrypting said physical characteristic information using said password as a cryptographic key and

outputting a cryptogram," as recited in independent claim 13.

Thus, even assuming, arguendo, that Buffam and Raike were combined, the combination would be silent as to providing the claimed features of the recording and/or reproducing unit recited in independent claim 13.

Because independent claims 14-15 and 24-26 include similar claim features as those recited in independent claim 13, although of different scope, the arguments presented above supporting the patentability of independent claim 13 are incorporated herein to support the patentability of independent claims 14-15 and 24-26.

In view of the foregoing, it is respectfully asserted that independent claims 13-15 and 24-26 are patentable in view of Buffam and Raike. Accordingly, it is respectfully requested that independent claims 13-15 and 24-26 be allowed.

CONCLUSION:

In accordance with the foregoing, it is respectfully submitted that all outstanding objections and rejections have been overcome and/or rendered moot, and further, that all pending claims patentably distinguish over the prior art. Thus, there being no further outstanding objections or rejections, the application is submitted as being in condition for allowance, which action is earnestly solicited.

If the Examiner has any remaining issues to be addressed, it is believed that prosecution can be expedited by the Examiner contacting the undersigned attorney for a telephone interview to discuss resolution of such issues.

If there are any underpayments or overpayments of fees associated with the filing of this Amendment, please charge and/or credit the same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: _September 21, 2004_____ By: _____

Alicia M. Choi
Registration No. 46,621

1201 New York Avenue, NW, Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501